UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/752,420	01/05/2004	Gregory Gordon Rose	030010	3858

23696 7590 04/24/2007	EXAMINER
QUALCOMM INCORPORATED 5775 MOREHOUSE DR. SAN DIEGO, CA 92121	KANE, CORDELIA P

	ART UNIT	PAPER NUMBER
	2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/24/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/24/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

		Application No.	Applicant(s)
Office Action Summary		10/752,420	ROSE ET AL.
		Examiner	Art Unit
		Cordelia Kane	2109

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 January 2004*.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)	5) ☐ Notice of Informal Patent Application
Paper No(s)/Mail Date *7/06/04* .	6) ☐ Other: _____ .

DETAILED ACTION

1.   This action is responsive to the non-provisional application filed on 12/31/03.

Claims 1 – 51 are pending. Claims 1, 11, 14, 19, 22, 26, 29, 33, 36, 40, 43, 47, 50 and

51 are independent.

Specification

2.   The disclosure is objected to because of the following informalities: On page 1,

paragraph's 11 and 12 the applicant seems to be misusing the terms private and public

key. The applicant refers to outputting the third public key once such that it can be

recreated, when I believe the applicant meant to disclose the private key to be

recreated. Also, the applicant refers to disabling the second key, and then using the

third key and then refers to recreating the second key and using it for authentication.

This process does not make sense. Finally, the applicant discloses outputting the

second public by creating at least two shares of the public key and outputting it to

separate entities. I believe the applicant meant to refer to splitting the private key into

shares.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

4.   Claims 2 , 7, 14 – 21, 23 and 36 – 42 are rejected under 35 U.S.C. 112, second

paragraph, as being indefinite for being unclear. Referring to claim 2, 15 and 23, the

applicant claims creating two shares of the second public key. It is unclear why the

applicant would divide a public key into two shares when the key has already been

made public. It is assumed that the applicant meant to distribute shares of the second

private key.

5.   Referring to claim 7, the applicant claims disabling a second private key, and

then recreating the second private key and using that for authentication. This is unclear

since the applicant just claimed to disable the second key. It is assumed that the

applicant meant to recreate the third private key and use it for authentication.

6.   Referring to claims 14 – 21 and 36 – 42, the applicant claims an apparatus but all

that is listed is software per se.

Claim Rejections - 35 USC § 101

7.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
> matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
> conditions and requirements of this title.

1.   Claims 14 – 21 and 36 – 42 are rejected under 35 U.S.C. 101 because the

claimed invention is directed to non-statutory subject matter. The claims lack the

necessary physical articles or objects to constitute a machine or a manufacture within

the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a

process nor are they a combination of chemical compounds to be a composition of

matter. As such, they fail to fall within a statutory category. They are, at best, functional

descriptive material per se.

2.   Descriptive material can be characterized as either "functional descriptive material" or "non-functional descriptive material." Both types of "descriptive material" are non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When <u>functional</u> descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

3.   Merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

Claim Rejections - 35 USC § 102

8.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

9.   Claims 1, 11, 14, 19, 22, 26, 50 and 51 are rejected under 35 U.S.C. 102(e) as being anticipated by Robert L. Hollis et al's US Patent 6,959,393. Referring to claim 1, Hollis teaches creating a first and second private and public key pair (column 24, lines 39-40). Both the second public and private key are outputted (column 24, line 41). It is inherent that the first private key would be used for authentication since it is not the backup.

10.   Referring to claim 14, Hollis teaches a system (column 5, line 61) for performing the method of claim 1, and therefor the apparatus of claim 14.

11.   Referring to claim 22, Hollis teaches that two computers are doing the communicating (column 3, line 40) as described in claim 1. Therefor Hollis teaches computer readable medium storing code as described in claim 22.

12.   Referring to claim 11, Hollis teaches:

    a.   Receiving a first public key (column 9, lines 63-64).

    b.   Receiving a second public key (column 10, lines 33-34).

    c.   Using the first public key for authentication (column 14, lines 38-40).

      d.   Using the second public key for authentication if the first public key fails (column 10, lines 31-36).

13.   Referring to claim 19, Hollis teaches a system (column 5, line 61) for performing the method of claim 11, and therefor the apparatus of claim 19.

14.   Referring to claim 26, Hollis teaches that two computers are doing the communicating (column 3, line 40) as described in claim 11. Therefor Hollis teaches computer readable medium storing code as described in claim 26.

15.   Referring to claim 50, Hollis teaches:

      e.   A processor for creating a first and second private and public key pair (column 24, lines 39-40).

      f.   A storage medium to store the first private key (column 9, line 55).

      g.   A transmitter to output the second private and public key pair (column 24, line 41) at the same time as the first public key (column 24, lines 43-44).

      h.   Using the first private key for authenticating is inherent from the fact that it is not the backup.

16.   Referring to claim 51, Hollis teaches:

      i.   Receiving a first public key (column 9, lines 64-65) and a second public key (column 10, lines 33-34).

      j.   A storage medium for storing both the first and second public keys (column 9, lines 59-61).

k.   A processor that knows to use the second public key when the first key

fails (column 10, lines 35-36). Using the first public key for authentication is

inherent from it not being the backup key.

17.   Claims 29, 30, 33, 34, 36, 37, 40, 41, 43, 44, 47 and 48 are rejected under 35

U.S.C. 102(e) as being anticipated by Joerg Schwenk's US Patent 7,162,037. Referring

to claim 29, Schwenk teaches creating a private (v) and public key (V) using a system

parameter (g) (column 4, line 43), then outputting the public key and the system

parameter (column 4, lines 43-45). While it is not specifically stated that g is outputted,

both entities have it so it can be inferred that it was outputted. The private key v is used

to create the public key V, therefor it is used for authentication.

18.   Referring to claim 36, Schwenk teaches that the entities are computer terminals

(column 3, lines 5-6) that are performing the method of claim 29 and therefor the

apparatus of claim 36.

19.   Referring to claim 43, Schwenk teaches that the two entities are computer

terminals (column 3, lines 5-6) that are performing the method as described in claim 29.

Therefor Hollis teaches computer readable medium storing code as described in claim

43.

20.   Referring to claim 30, Schwenk teaches creating a new private key C using the

previous private key v and the system parameter (column 4, lines 56-59). The system

parameter g is used to calculate R and therefor S, which is then used to calculate C.

The secret key is used for authentication (column 4, line 53-54).

21.   Referring to claim 37, Schwenk teaches that the entities are computer terminals (column 3, lines 5-6) that are performing the method of claim 30 and therefor the apparatus of claim 37.

22.   Referring to claim 44, Schwenk teaches that the two entities are computer terminals (column 3, lines 5-6) that are performing the method as described in claim 30. Therefor Hollis teaches computer readable medium storing code as described in claim 44.

23.   Referring to claim 33, Schwenk teaches receiving a public key V, and a system parameter g (column 4, lines 43-45). The public key is used for authenticating in that it is used to derive the seed value to be used for the future public key (column 2, lines 59-63). Schwenk goes on to teach the generation of a new public key U using the seed value S after the loss of a key (column 3, lines 59-61). The seed value S is derived from the system parameter g and the public key V, therefor the public key and system parameter are used to generate the new public key. It is inherent that the public key would have failed otherwise the system would not know that the key had been lost or compromised.

24.   Referring to claim 40, Schwenk teaches that the entities are computer terminals (column 3, lines 5-6) that are performing the method of claim 33 and therefor the apparatus of claim 40.

25.   Referring to claim 47, Schwenk teaches that the two entities are computer terminals (column 3, lines 5-6) that are performing the method as described in claim 33.

Therefor Hollis teaches computer readable medium storing code as described in claim

47.

26.   Referring to claim 34, Schwenk teaches generating a new public key U using the

seed value S (column 2, lines 59-63) which is derived using powers of the previous

public key V (Figure 1). It is inherent that the public key that works would be accepted.

27.   Referring to claim 41, Schwenk teaches that the entities are computer terminals

(column 3, lines 5-6) that are performing the method of claim 34 and therefor the

apparatus of claim 41.

28.   Referring to claim 48, Schwenk teaches that the two entities are computer

terminals (column 3, lines 5-6) that are performing the method as described in claim 34.

Therefor Hollis teaches computer readable medium storing code as described in claim

48.

Claim Rejections - 35 USC § 103

29.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

30.   The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.

      2.   Ascertaining the differences between the prior art and the claims at issue.

      3.   Resolving the level of ordinary skill in the pertinent art.

      4.   Considering objective evidence present in the application indicating obviousness or nonobviousness.

31.   Claims 2 – 10, 15 – 18, and 23 – 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollis and further in view of Bruce Schneier's Applied Cryptography. Hollis teaches all the limitations of the parent claim, but fails to teach the splitting of the second public key into shares. Schneier goes on to teach that it is the best method to split the key into pieces and share the key between different entities (page 182, 1st and 2nd paragraph). It would have been obvious to modify Hollis to separate the backup key into different parts and distribute to different entities, as taught by Schneier, because it is more secure.

32.   Referring to claim 15, Hollis teaches a system (column 5, line 61) for performing the method of claim 2, and therefor the apparatus of claim 15.

33.   Referring to claim 23, Hollis teaches that two computers are doing the communicating (column 3, line 40) as described in claim 2. Therefor Hollis teaches computer readable medium storing code as described in claim 23.

34.   Referring to claim 3, Hollis teaches using the second private key for authentication (column 10, line 23). It fails to teach the recreation of the second private key. Schneier teaches that separating the keys is a better way to secure backup keys and that when it comes time to use them that you have to reconstruct them (page 182 second paragraph). It would have been obvious to modify Hollis to reconstruct the keys, as taught by Schneier, because it is a more secure way to store the backup key.

35.   Referring to claim 16, Hollis teaches a system (column 5, line 61) for performing

the method of claim 3, and therefor the apparatus of claim 16.

36.   Referring to claim 24, Hollis teaches that two computers are doing the

communicating (column 3, line 40) as described in claim 3. Therefor Hollis teaches

computer readable medium storing code as described in claim 24.

37.   Referring to claim 4, Hollis teaches disabling the first private key when the

second is used for authentication (column 14, lines 46-48).

38.   Referring to claim 25, Hollis teaches that two computers are doing the

communicating (column 3, line 40) as described in claim 4. Therefor Hollis teaches

computer readable medium storing code as described in claim 25.

39.   Referring to claim 5, Hollis teaches the creation of a primary key and a backup

key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a

third private and public key pair, once the backup key had been used since there would

need to be a new backup. It also would have been obvious to then distribute the new

backup public key.

40.   Referring to claim 17, Hollis teaches a system (column 5, line 61) for performing

the method of claim 5, and therefor the apparatus of claim 17.

41.   Referring to claim 6, Hollis teaches using the third private key for authentication

(column 10, line 23). He fails to teach the outputting of the third key in separate pieces.

Schneier teaches that it is a more secure method with backup keys (third key) to split it

into separate parts and distribute them to different entities, which is the same as

outputting it so that it can be recreated. He goes on to teach how then the pieces can

then be brought back together to be recreated (page 182, second paragraph). It would

have been obvious to modify Hollis to split the key into separate pieces since it is a

more secure method for backup keys.

42.   Referring to claim 7, Hollis teaches disabling the original (second) private key

(column 14, lines 46-48). Hollis goes on to teach using the third private key for

authentication (column 10, line 23). It fails to teach the recreation of the third private

key. Schneier teaches that separating the keys is a better way to secure backup keys

and that when it comes time to use them that you have to reconstruct them (page 182

second paragraph). It would have been obvious to modify Hollis to reconstruct the keys,

as taught by Schneier, because it is a more secure way to store the backup key.

43.   Referring to claim 8, Hollis teaches the creation of a primary key and a backup

key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a

third private and public key pair, once the backup key had been used since there would

need to be a new backup. It would also be obvious to repeat that process again and

create a fourth backup pair of keys. It would then be inherent to distribute both new

public keys. Schneier teaches distributing pieces of a private key to be used for

recreation later (page 182, second paragraph). Since the fourth key pair would now be

the backup, it would have been obvious to modify Hollis so that it distributes pieces of

the fourth private key for recreation later since it is a more secure way to store backups.

44.   Referring to claim 18, Hollis teaches a system (column 5, line 61) for performing

the method of claim 8, and therefor the apparatus of claim 18.

45.   Referring to claim 9, Hollis teaches using a new (third) private key for

authentication (column 10, line 23). He goes on to teach the disabling of the old

(second) key for authentication (column 14, lines 46-48).

46.   Referring to claim 10, Hollis teaches using a new (fourth) private key for

authentication (column 10, line 23). It fails to teach the recreation of the fourth private

key. Schneier teaches that separating the keys is a better way to secure backup keys

and that when it comes time to use them that you have to reconstruct them (page 182

second paragraph). It would have been obvious to modify Hollis to reconstruct the keys,

as taught by Schneier, because it is a more secure way to store the backup key.

47.   Claims 12, 13, 20, 21, 27 and 28 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Hollis. Referring to claim 12, Hollis teaches the creation of a primary

key and a backup key (column 24, lines 39-41). It would have been obvious to modify

Hollis to create a third private and public key pair, once the backup (second) key had

been used, as taught by Hollis (column 10, line 23), since there would need to be a new

backup. It would have been obvious that after creation of the new backup key pair to

distribute the new (third) public key since it would be needed for future authentication.

48.   Referring to claim 20, Hollis teaches a system (column 5, line 61) for performing

the method of claim 12, and therefor the apparatus of claim 20.

49.   Referring to claim 27, Hollis teaches that two computers are doing the

communicating (column 3, line 40) as described in claim 12. Therefor Hollis teaches

computer readable medium storing code as described in claim 27.

50.   Referring to claim 13, Hollis teaches the creation of a primary key and a backup
key (column 24, lines 39-41). It would have been obvious to modify Hollis to create a
third private and public key pair, once the backup key had been used since there would
need to be a new backup. It would also be obvious to repeat that process again and
create a fourth backup pair of keys. It would have been obvious to then distribute the
third and fourth public keys since they would be needed for future authentication.

51.   Referring to claim 21, Hollis teaches a system (column 5, line 61) for performing
the method of claim 13, and therefor the apparatus of claim 21.

52.   Referring to claim 28, Hollis teaches that two computers are doing the
communicating (column 3, line 40) as described in claim 13. Therefor Hollis teaches
computer readable medium storing code as described in claim 28.

53.   Claims 31, 32, 35, 38, 39, 42, 45, 46, and 49 are rejected under 35 U.S.C. 103(a)
as being unpatentable over Schwenk and further in view of Liao et al's US Patent
6,263,437. Schwenk teaches the limitations of the parent claim. It fails to teach the use
of a counter value. Liao teaches the use of a counter value to keep track of the
generations of key regeneration (column 15, line 59-61). It would have been obvious to
modify Schwenk to include a counter value, as taught by Liao, because it would be
more efficient to keep track of how many iterations have been through.

54.   Referring to claim 38, Schwenk teaches that the entities are computer terminals
(column 3, lines 5-6) that are performing the method of claim 31 and therefor the
apparatus of claim 38.

55.   Referring to claim 45, Schwenk teaches that the two entities are computer

terminals (column 3, lines 5-6) that are performing the method as described in claim 31.

Therefor Hollis teaches computer readable medium storing code as described in claim

45.

56.   Referring claim 32, Schwenk teaches creating a new private key C using the

previous private key v and the system parameter (column 4, lines 56-59). The system

parameter g is used to calculate R and therefor S, which is then used to calculate C.

The secret key is used for authentication (column 4, line 53-54). Schwenk fails to teach

using a counter in the calculation. Liao teaches the use of a counter value to keep track

of the generations of key regeneration (column 15, line 59-61). It would have been

obvious to modify Schwenk to include a counter value, as taught by Liao, because it

would be more efficient to keep track of how many iterations have been through.

57.   Referring to claim 39, Schwenk teaches that the entities are computer terminals

(column 3, lines 5-6) that are performing the method of claim 32 and therefor the

apparatus of claim 39.

58.   Referring to claim 46, Schwenk teaches that the two entities are computer

terminals (column 3, lines 5-6) that are performing the method as described in claim 32.

Therefor Hollis teaches computer readable medium storing code as described in claim

46.

59.   Referring to claim 35, Schwenk teaches receiving a public key V, and a system

parameter g (column 4, lines 43-45). Schwenk goes on to teach the generation of a new

public key U using the seed value S after the loss of a key (column 3, lines 59-61). The

seed value S is derived from the system parameter g and the public key V, therefor the public key and system parameter are used to generate the new public key. Schwenk fails to teach using a counter in the calculation. Liao teaches the use of a counter value to keep track of the generations of key regeneration (column 15, line 59-61). It would have been obvious to modify Schwenk to include a counter value, as taught by Liao, because it would be more efficient to keep track of how many iterations have been through.

60.   Referring to claim 42, Schwenk teaches that the entities are computer terminals (column 3, lines 5-6) that are performing the method of claim 35 and therefor the apparatus of claim 42.

61.   Referring to claim 49, Schwenk teaches that the two entities are computer terminals (column 3, lines 5-6) that are performing the method as described in claim 35. Therefor Hollis teaches computer readable medium storing code as described in claim 49.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cordelia Kane whose telephone number is 571-272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CPK 3/29/07

KIMBERLY D. NGUYEN
PRIMARY EXAMINER